REMARKS

This Amendment is submitted in reply to the Final Office Action dated June 25, 2010 and the Advisory Action dated September 1, 2010. Applicant respectfully requests reconsideration and further examination of the patent application pursuant to 37 C.F.R. § 1.111.

Summary of the Examiner's objections and rejections

The Specification stands objected to as failing to provide proper antecedent basis for the claimed subject matter.

Claims 54-57 and 60-62 stand rejected under 35 U.S.C. § 112 (second paragraph) as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 54-57 and 60-62 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Gruse (US 6,389,538).

Summary of claim amendments

Applicant has amended claim 60 to correct an antecedent error. In addition, Applicant has added new claims 68-69 where the support for these new claims can be found in pending claims 54 and 57 and in original claim 13 of the originally filed PCT patent application. No new subject matter has been added.

Remarks regarding objected specification

The Specification stands objected to as failing to provide proper antecedent basis for the claimed subject matter "means for performing a security operation to cryptographically link said usage information with a particular user account or identity". Applicant respectfully traverses this rejection in that the antecedent support for this claimed limitation is provided on page 4, lines 1-2 (describes linking) and page 4, lines 12-23 (describes cryptography) of the originally filed PCT patent application. Accordingly, Applicant respectfully requests the removal of this objection.

Remarks regarding the §112 (second paragraph) rejections

Claims 54-57 and 60-62 stand rejected under 35 U.S.C. § 112 (second paragraph) because the claimed element "means for performing a security operation to cryptographically link said usage information with a particular user account or identity" is a means plus function limitation that invokes 35 U.S.C. 112, sixth paragraph but the written description fails to disclose the corresponding structure, material, or acts for the claimed function. Applicant respectfully traverses the pending § 112 (second paragraph) rejection.

The Federal Circuit has stated that the test for meeting the definiteness requirement to support claim limitations which invoke 35 USC 112 (sixth paragraph) is that the corresponding structure (or material or acts) of a means (or step)-plus-function limitation must be disclosed in the specification itself in a way that one skilled in the art will understand what structure (or material or acts) will perform the recited function. See Atmel Corp. v. Information Storage Devices, Inc., 198 F.3d 1374, 1381, 53 USPQ2d, 1225, 1230 (Fed. Cir. 1999). See also MPEP 2181 II. In fact, the Federal Circuit has indicated that while the specification must contain structure linked to the claimed means, this is not a high bar since "[a]ll one needs to do...is to recite some structure corresponding to the means in the specification...so that one can readily ascertain what the claim means and comply with the particularity requirements of [§ 112] Para. 2". Additionally, interpretation of what is disclosed in the specification must be made in light of the knowledge of one skilled in the art. Thus, in order for a means-plus-function claim to be valid under § 112, the corresponding structure of the limitation "must be disclosed in the written description in such a manner that one skilled in the art will know and understand what structure corresponds to the means limitation. Otherwise, one does not know what the claim means". See Biomedino, LLC v. Waters Technology Corp., 490, F.3d 946 (Fed. Cir. 2007) and see also Atmel, 198 F.3d at 1382, 53 USPQ2d at 1230. Furthermore, the Federal Circuit has also referred to the term "computer" as being a "magic word" that can satisfy the requirements of Section 112, Para. 2. See In re Dossel, 115 F.3d 942, 946-947, 42 USPQ2d 1881, 1885 (Fed. Cir. 1997).

In the present application, one skilled in the art would readily recognize that the function of the claimed element "means for performing a security operation to cryptographically link said usage information with a particular user account or identity" is associated with the security operation unit 160, authenticator 160, and/or the authentication and key agreement (AKA) module 460 which if the claimed function is not performed by these units themselves then it can be performed by anyone of the following devices: the mobile unit or mobile phone 10 (inherently has a computer-processor and memory), the computer, the subscriber identity module (SIM) 400, the tamper resistant device 400, or the DRM agent 430. These devices have been described and illustrated on page 35, line 14 through page 38, line 29, original claim 13, and FIGURES 2, 4, 5, 7, 8, and 9 in the originally filed PCT patent application.

Alternatively, the Federal Circuit has even held that without the use of the magic word "computer" or "computer code" the disclosure can still satisfy the requirements of Section 112, Para. 2. In particular, the Federal Circuit in the In re Dossel case discussed where the function recited in the means-plus-function limitation involved "reconstructing" data. The issue was whether the structure underlying this "reconstructing" function was adequately described in the written description to satisfy 35 U.S.C. 112, second paragraph. The court stated that "[n]either the written description nor the claims use the magic word "computer", nor do they quote computer code that may be used in the invention. Nevertheless, when the written description is combined with claims 8 and 9, the disclosure satisfies the requirements of Section 112, Para. 2." The court concluded that based on the specific facts of the case, one skilled in the art would recognize the structure for performing the "reconstructing" function since "a unit which receives digital data, performs complex mathematical computations and outputs the results to a display must be implemented by or on a general or special computer." See Dossel, 115 F.3d at 946-47, 42 USPQ2d at 1885.

In this regard, Applicant respectfully submits that one skilled in the art would readily recognize the structure for performing the "performing a security operation to cryptographically link said usage information with a particular user account or identity"

function namely the security operation unit 160, the authenticator 160 and/or the AKA module 460 receives digital data, performs complex mathematical computations, and outputs the results and as such must be implemented by or on a general or special computer. In view of at least the two foregoing arguments, the Applicant respectfully submits that the pending claims 1-11 and the originally filed specification satisfy the definiteness requirement of 112 (second paragraph) when 112 (sixth paragraph) is invoked.

Remarks regarding the §103(a) rejections

Applicant respectfully traverses the obviousness rejection of the pending independent claim 54 in view of Gruse. The pending independent claim 54 recites the following:

> 54. Client system capable of using digital content provided by a content provider over a network, said content-using client system comprising:
> receiving agent for receiving certain digital content from said content provider;
> rendering device for rendering said received digital content;
> logging agent for monitoring usage information concerning the actual rendering of said digital content by said rendering agent; and
> means for performing a security operation to cryptographically link said usage information with a particular user account or identity (emphasis added).

The Examiner's closest prior art Gruse teaches the following:

> A system for tracking usage of digital content on user devices. Electronic stores coupled to a network sell licenses to play digital content data to users. Content players, which receive from the network the licensed content data, are used to play the licensed content data. Additionally, a logging site that is coupled to the network tracks the playing of the content data. In particular, the logging site receives play information from the network, and the play information includes the number of times that the content data has been played by the associated content player. Also provided is a method for tracking usage of digital content on user devices. According to the method, a license to play digital content data is sold to a user, and the licensed content data is transmitted to a content player for the user. Further, information is transmitted to a logging site whenever the content data is played by the content player or copied from the content player to an external medium so that usage of the licensed content data can be tracked.

(see abstract)

The Examiner is correct in that Gruse discloses or at least suggests the receiving agent, the rendering agent, and the logging agent as recited in the pending independent claim 54. However, the Examiner is not correct in stating that Gruse suggests the claimed limitation "means for performing a security operation to cryptographically link said usage information with a particular user account or identity". The substantial difference between the present invention and Gruse with respect to the claimed "means for performing a security operation to cryptographically link said usage information with a particular user account or identity" should become readily apparent in the following discussion.

In the Final Office Action, the Examiner in referring to the claimed "means for performing a security operation to cryptographically link said usage information with a particular user account or identity" stated the following:

> means for performing a security operation to cryptographically link information with a particular user account or identity (see description of means for creating containers and Digital Signatures in at least c. 16, ll. 1+).
>
> 24. Gruse does not directly disclose means for performing a security operation to cryptographically link said usage information with a particular user account or identity.
>
> 25. However, it would have been obvious to one of ordinary skill in the art, at the time the invention was made, to use the means for performing a security operation (i.e., the components that create a digital signature), as disclosed by Gruse, to cryptographically link the usage information of Gruse with a particular user identity. One would have been motivated to do so because such link would provide the receiving facility to Gruse with assurance of the integrity of the usage information (see Gruse, at least c. 27, ll. 20-23).

(see pages 6-7 in Final Office Action)

Applicant respectfully submits that the Examiner's motivation for modifying Gruse to read-on the claimed invention is misplaced. Gruse explains that an exemplary use of the usage information is to determine the popularity of a content (see col. 89, lines 23-25). However, Gruse is deficit in showing a cryptographically link (i.e., trustworthy binding) of usage information to a particular user account or identity. Although Gruse mentions that an identity of a user of content may be attached to the usage information

nothing is said how a cryptographically link, e.g., trustworthy binding, is achieved. Instead, Gruse discloses signing of information with a digital signature of the end-user device and more precisely the signing of a Secure Container (SC) (see c. 26, ll. 20-22). Gruse defines a Secure Container in general to be a cryptographic carrier of information or content that uses encryption, digital signatures, and digital certificates to provide protection. In particular, Gruse defines a Secure Container as follows:

> Secure Containers are used to distribute encrypted content and information among the system components. A SC is a cryptographic carrier of information or content that uses encryption, digital signatures, and digital certificates to provide protection against unauthorized interception or modification of electronic information and content. It also allows for the verification of the authenticity and integrity of the Digital Content. The advantage of these rights management functions is that the electronic Digital Content distribution infrastructure does not have to be secure or trusted. Therefore allowing transmission over network infrastructures such as the Web and Internet. This is due to the fact that the Content is encrypted within Secure Containers and its storage and distribution are separate from the control of its unlocking and use. Only users who have decryption keys can unlock the encrypted Content, and the Clearinghouse(s) releases decryption keys only for authorized and appropriate usage requests. The Clearinghouse(s) will not clear bogus requests from unknown or unauthorized parties or requests that do not comply with the content's usage conditions as set by the content proprietors. In addition, if the SC is tampered with during its transmission, the software in the Clearinghouse(s) determines that the Content in a SC is corrupted or falsified and repudiate the transaction.
>
> (see col. 10, lines 9-33)

As can be seen, Gruse teaches the encryption of Secure Containers which contain content but there is no teaching where one piece of content (claimed usage information) is cryptographically linked to another piece of content (claimed particular user account or identity). Thus, Gruse's Secure Containers can not be used to resolve disputes between a user and a content provider regarding the usage of content. In contrast, the present invention with the claimed cryptographically linking of the usage information and the particular user account or identity is desirable in that the content provider now has the "trustworthy" information it needs to determine if a user is being dishonest when repudiating their usage information. Therefore, there is no hint in Gruse to suggest the claimed "means for performing a security operation to cryptographically

link said usage information with a particular user account or identity". In view of at least the foregoing, Applicant respectfully submits that the aforementioned substantial difference between the pending independent claim 54 and Gruse is indicative of the patentability of the pending independent claim 54 and the corresponding dependent claims 55-57 and 60-62.

Referring now to the pending dependent claim 57, Applicant respectfully submits that this claim is not disclosed or suggested by Gruse. The pending dependent claim 57 recites the following:

> 57. The client system according to claim 54, wherein said usage information comprises a representation of said client-rendered digital content and rendering quality information (emphasis added).

In rejecting the pending dependent claim 57, the Examiner cited the following section of Gruse:

> 3. Copy/Play Management Components 1504
>
> These components handle set up of encryption keys, Watermark processing, Copy management, and more. Interfaces also exist for communication with the Clearinghouse(s) 105, transmission of purchase requests, and more, for special services such as pay per listen or cases where each access to the Content 113 is accounted for. Currently, the communications to the Clearinghouse(s) 105 functions are handled by the SC(s) Processor 192.
>
> The use of the Content 113 by the Player Applications 195 on End User Device(s) 109 is logged into a database such as the License Database 197. The tracking of each use of Content 113 by the Player Application 195 can be transmitted to one or more logging sites such as the Clearing House(s) 105 or Content Provider(s) 101 or Electronic Digital Content Store(s) 103 or any site designated and coupled to Transmission Infrastructures 107. This transmission can be scheduled at predetermined times to upload the usage information to a logging site. One predetermined time contemplated is early in the morning when Transmission Infrastructures 107 may not be as congested with network traffic. The Player Application 195 using known techniques, wakes-up at a scheduled time, and transmit the information from the local logging database to the logging site. By reviewing the logging site information, the Content Provider(s) 101 can measure the popularity of their Content 113.
>
> In another embodiment, the instead of logging the usage of Content 113 for later uploading to a logging site, the use of the Content 113 is uploaded to the logging

> site during every use of the Content 113. For example, when duplicating or copying the Content 113 stored at the End User Device(s) 109, on to an external device such as DVD Disc, digital tape, flash memory, mini Disc or equivalent read/writeable removable media, the use is updates to the logging site. This may be a precondition to copying the Content 113 in the usage conditions 206 that is transmitted when the Content 113 is purchased. This ensures the Content Provider(s) 101 can accurately track the usage of their Content 113 during their playing, duplicating or other actions upon the Content 113.
>
> In addition, other information about the Content 113 can be uploaded to the logging site. For example the last time (e.g., hour and day) the Content 113 was performed; how many times the Content 113 was performed; if the Content 113 has been duplicated or copied to an authorized external device such as DVD Disc, digital tape or mini-Disc. In cases where there are multiple distinct users of a single Player Application 195 on the End User Device(s) 109, such as different members of a family, the identifications of the user of the Content 113 is transmitted along with the usage information to the logging site. By reviewing the usage information uploaded to the logging site, the Content Provider(s) 101 can measure the popularity of the Content 113 base on the actual usage, the identification of the user and the number of times the Content 113 has been performed. The actual usage measurement makes this system more factual driven over systems using sampling methods, such as a Nielsen Rating scheme for televisions, or telephone surveys, where only a limited number of users are sampled at any one time and the results extrapolated. In this present embodiment, the actual usage can be measures for the users logging back onto a designated web site such as the Electronic Digital Content Store(s) 103 or Content Provider(s) 101.

(see col. 88, line 40 through col. 89, line 35).

As can be seen, Gruse's usage information includes: (1) number of times content is played; (2) when content is duplicated or copied to an external device; (3) actual time and day the content was performed; and (4) identification of distinct users of the content. There is no disclosure whatsoever in Gruse where the usage content includes the claimed "rendering quality information". As discussed above, the present invention with the claimed cryptographically linking of the usage information and the particular user account or identity is desirable in that the content provider now has the "trustworthy" information it needs to determine if a user is being dishonest when repudiating their usage information. In view of pending dependent claim 57, the content provider will now have "rendering quality information" which it can use to determine if the user is being dishonest when the state that the quality of the rendered content was sub-standard. Accordingly, Applicant respectfully submits that the aforementioned

substantial difference between the pending dependent claim 57 and Gruse is indicative of the patentability of the pending dependent claim 57.

Examiner's claim interpretation

Applicant respectfully submits that regardless of the Examiner's claim interpretations the pending independent claim 54 and the corresponding dependent claims 55-57 and 60-62 are still patentable in view of Gruse.

Remarks regarding the new claims 68-69

Applicant respectfully submits that the new independent claim 68 and new dependent claim 69 are patentable in view of Gruse. The new independent claim 68 and new dependent claim 69 are as follows:

> 68. Client system that uses digital content provided by a content provider over a network, said content-using client system comprising:
> receiving agent that receives certain digital content from said content provider;
> rendering agent that renders said received digital content;
> logging agent that monitors usage information concerning the actual rendering of said digital content by said rendering agent; and
> authenticator that performs a security operation to cryptographically link said usage information with a particular user account or identity.
>
> 69. The client system according to claim 68, wherein said usage information comprises a representation of said client-rendered digital content and rendering quality information.

The new independent claim 68 and new dependent claim 69 recite claim limitations that do not invoke 112 (sixth paragraph) and hence satisfy the definiteness requirement of 112 (second paragraph). In addition, the new independent claim 68 and the new dependent claim 69 recite the same or similar distinguishing limitations that have been discussed above with respect to pending claims 54 and 57. As such, the aforementioned remarks regarding the patentability of pending claims 54 and 57 apply as well to the new claims 68 and 69. Accordingly, Applicant respectfully submits that the new claims 68 and 69 are patentable over Gruse.

CONCLUSION

In view of the foregoing remarks, Applicant believes all of the claims currently pending in the application to be in a condition for allowance. Therefore, Applicant respectfully requests that the Examiner withdraw all objections and rejections and issue a Notice of Allowance for pending claims 54-57, 60-62, and 68-69.

The Commissioner is hereby authorized to charge any fees for this paper to Deposit Account No. 50-1379.

Applicant requests a telephonic interview if the Examiner has any questions or requires any additional information that would further or expedite the prosecution of the Application.

Respectfully submitted,

/William J. Tucker/

By William J. Tucker
Registration No. 41,356

Date: September 23, 2010

Ericsson Inc.
6300 Legacy Drive, M/S EVR 1-C-11
Plano, Texas 75024

(214) 324-7280 or (972) 583-2608
william.tucker@ericsson.com